ENCLAVE

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 3, Release 1

28 July 2005

Developed by DISA for the DOD

This page is intentionally left blank.

SUMMARY OF CHANGES

General Changes:

Title Page – Changed the Title. Removed the word "Security" after Enclave.

Corrected grammatical errors.

Corrected DOD Ports, Protocols, and Services references throughout the document.

Removed the Glossary of Terms Appendix.

Added Appendix B – Data Center Enclave.

Specific Changes:

Section 1. INTRODUCTION

Changed Non-classified to Unclassified.

Section 1.5 Information Assurance Vulnerability Management (IAVM)

Added the word notices to IAVM.
Changed bullets to DOD rather than DISA specific requirements.

Section 1.10.1 General Business LAN

Changed the type of Enclave to "General Business LAN" vice Office LAN.

Section 2.6 Patch Management

Added a bullet to require testing of patches in a non-production environment.
Added "from a secure source or trusted site" to EN042.

Section 2.7.1

Added that the DAA at each site must approve risky/Red traffic through a VPN.
Reorganized 3rd paragraph.

Section 2.7.2

Added "Network" in front of IDS; clarified the use of application proxy requirement.

Section 2.7.2.1

Added, "When the VPN connects enclaves owned by more than one DAA, each must approve the connection."

Section 2.7.2.2 Minimum Enclave Requirements

Added DOD 8551.1 as a reference. Added "both ingress and egress filtering" for the DDOS ports.

Section 2.7.2.4 Virtual Private Network (VPN) Encryption

Removed "VPNs are an acceptable solution for networking applications using ports or protocols that are no longer authorized based on requirements in this STIG."

Section 2.9 Port Security

Added that 802.1x has not yet been approved for use on the SIPRNet.

Section 2.10 FTP and Telnet

New Section FTP/Telnet. Removed AORL attachment statement.

Section 2.11 Enclaves Supporting VoIP and VTC systems

Added verbiage on networks or enclaves supporting VoIP and VTC systems.

Section 3.2.1 Internet Applications (Web Servers)

Update web section to incorporate changes based on new policy and Web STIG requirements.

Section 3.2.3 Mobile Code

1st paragraph, added "by the recipient."

Section 3.3 Wireless Devices

Changed 802.1x to 802.11.
Assigned PDI to first bullet.
Added EN745 requirement to ensure a policy is in place to scan for rogue wireless devices.

Section 4. Vulnerability Assessments

Reworded EN790.

Section 5.2 Recommendations

Assigned PDI to requirement.

Section 5.3 Ports and Protocols

Added two-factor authentication to the first paragraph.

This page is intentionally left blank.

TABLE OF CONTENTS

LIST OF TABLES

APPENDICES

This page is intentionally left blank.

1. INTRODUCTION

This Security Technical Implementation Guide (STIG) on Enclave security provides the information protection guidance necessary to implement secure Information Systems (ISs) and networks while ensuring interoperability.

Department of Defense (DOD) ISs must have adequate safeguards, both technical and procedural, to ensure the security of data processed. In general, DOD ISs must provide maximum feasible safeguards to achieve the highest level of security possible. The actual safeguards used will be commensurate with the operational requirements, information sensitivity level, and consequences of exploitation of the specific DOD IS.

The majority of DOD ISs are connected to Local Area Networks (LANs) and use Wide Area Networks (WANs) (e.g., the Unclassified Internet Protocol Router Network [NIPRNet] or Secret Internet Protocol Router Network [SIPRNet]) as the primary data transport mechanism. Unfortunately, an adversary attempting to compromise DOD information and ISs can exploit these LAN/WAN connections. Providing an adequate level of information protection at an acceptable cost is difficult in this type of environment. This document is aimed at identifying mitigating controls to aid in securing and protecting the perimeter and computing environment and achieving the objectives as identified in the Department of Defense Directive, "Information Assurance, 8500.1," and the Department of Defense Instruction, "Information Assurance (IA) Implementation, 8500.2."

1.1 Purpose

The network and resources of a DOD agency must provide secure, obtainable, and reliable services and data to all customers, DOD users, and most importantly, the warfighter. In order to gain secure reliable services; confidentiality, integrity, availability, and non-repudiation controls must be employed. The purpose of this STIG is to assist sites in meeting the minimum requirements, standards, controls, and options for securing the enclave as a whole and providing technical guidance to secure specific enclave components in detail.

1.2 Authority

DOD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with the Director, NSA." This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing unclassified but sensitive information.

1.3 Scope

This document applies to all DOD administered or managed enclaves or security domains. The requirements set forth in this document are designed to assist Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs), in support of protecting DOD network infrastructures and resources. This document will also assist in identifying external security exposures created when the site is connected to at least one IS outside the site's control.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" implies mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This will make all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" is considered a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Information Assurance Vulnerability Management (IAVM)

The DOD has mandated that all IAVM notices are received and acted on by all commands, agencies, and organizations within the DOD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert.

- *(EN010: CAT II) The IAO will ensure all assets and/or systems that support enclave protection are registered with an IAVM tracking mechanism (e.g., Vulnerability Management System (VMS)).*

- *(EN020: CAT III) The IAM will ensure DOD sites that utilize an IAVM tracking tool designate their SAs who are responsible for critical assets, and in addition, are registered.*

- *(EN030: CAT II) The IAO and IAM, in coordination with the SA, are responsible for ensuring that all IAVM notices are responded to within the specified period of time.*

1.6 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1-1. Vulnerability Severity Code Definitions

1.7 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.8 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to **fso_spt@disa.mil**. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

1.9 Definitions

This STIG defines an enclave security architecture as an integrated system supporting Defense-in-Depth (DID). An enclave includes the "Enclave Perimeter" and "Computing Environment" layers in the DID architecture which includes all components of the network, application, and host layers. If the network traverses different security levels (unclassified to classified), then Secret and Below Interoperability (SABI) documents and appropriate Points of Contact (POCs) need to be reviewed/contacted to determine the proper security requirements. Examples of enclaves within DOD are the Computing Services System Management Centers (SMCs), Processing Elements (PEs), Network Operations Center (NOC), and Theater Network Center (TNC). The DISANET consists of multiple enclaves connected through the NIPRNet.

> "An Enclave is the collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the automated information system (AIS) applications or outsourced IT-based processes they

> support, and derive their security needs from those systems. They provide standard IA capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the application they host, backbone networks, and data processing centers." (DODD 8500.1 E2.1.16.2)

An enclave perimeter includes those points where non-members of an enclave gain access to resources and information within that enclave, or where members of the enclave, but not resident within the enclave, gain access to resources or information within that enclave. This includes those points at which the enclave connects to any WAN service, and those points where members of that enclave obtain dial-up or remote access.

Enclaves can be broken down into Security Domains or Communities of Interest (COIs). A security domain or COI is considered a sub-enclave, meaning that it derives it connectivity via another enclave. This STIG is based on the user community, general access requirements, the type of data that traverses the network and stored on systems, and assumed threats. In addition, all the security-related functions within a security domain should be essentially identical. An example would be two sections of an organization that use the same security policy, but have different sets of SAs and separate authentication databases. Even though the same security policy is in use in both sections, these two sections are actually separate security domains. A security domain would require a firewall system at a LAN-to-LAN interface, in addition to the firewall separating the LANs from the WAN at the enclave perimeter.

Backdoor service or access that avoids the use of DOD approved security tools, products, and security processes is prohibited unless approved through the DOD waiver process. The following site has information regarding NIPRNet access and approved gateway connections: https://snap.dod.mil.

1.10 Enclave Types

There are various categories of enclaves as a result of customer, architectural, and mission requirements. Larger backbone type enclaves, such as the Defense Information System Network (DISN), are actually comprised of numerous network enclaves and site facility enclaves. Certification and Accreditation (C&A) efforts should specify the type of enclave certification as site or network and be clearly identified with boundaries.

The types of enclaves addressed in this STIG are defined below and as requirements are set forth in future releases, the enclave for which they are required will be identified.

NOTE: The NOC and Test and Development enclaves are referenced in this release; however, security and architectural requirements are currently being addressed and will be consolidated and enumerated in updates to this document.

1.10.1 General Business LAN Enclave

A general business LAN (to include administrative and headquarters) enclave is a traditional, user-based environment, which maintains a connection or connections to the NIPRNet or SIPRNet, and a security domain. A general business LAN enclave provides minimal services to the outside world and the primary role is to provide services to internal users as it provides limited or no publicly accessible resources. The primary function of a general business LAN enclave is to provide resources such as printing, e-mail, Internet access, etc., to users internal to the network infrastructure. A general business LAN enclave is an organization with controlled assets and is best represented as an organization performing a single function with multiple managed elements operating under the same security policy.

1.10.2 Network Operations Center Enclave

A NOC may contain multiple enclaves to include an administrative subnet for user level services or resources and an operational subnet to remotely monitor and administer security and network devices. A NOC enclave is defined as a single site location that is performing management of multiple network enclave elements that may be based outside of traditional enclave boundaries. A NOC will often contain numerous sub-enclaves that are part of a distributed network enclave. This functionality is at a single site or facility for the infrastructure, and also for a distributed network infrastructure.

Establishment of requirements for a NOC enclave will be provided in an update to this document.

1.10.3 Data Center Enclave

A data center enclave is defined as an enterprise level network that services multiple sites. A data center may have numerous customers and users outside of the LAN enclave that need to access resources and it may also utilize management and control centers to remotely administer devices and hosts. The data center is not a traditional LAN enclave, rather it is a specialized enclave providing distributed, high-performance, MAC II application computing for globally distributed customers. This functionality is defined as a site facility enclave with the primary operational requirement for providing computing services on a large scale to many different customers.

Refer to Appendix B for Data Center security requirements. This Appendix to the Enclave STIG is For Official Use Only (FOUO) and will be maintained separately from this document.

1.10.4 Test and Development Enclave

Test and development or laboratory (LAB) enclaves are designed for the express purpose of design, installation, development, and testing of operating systems, applications, and configuration. A test and development enclave is defined as a sub-enclave within a site facility enclave that has a mission that is separate from the mission of the site facility enclave. The test and development enclave will often contain NOC enclave network and operating components that are used to manage the test and development enclave infrastructure. The test and development enclave is physically disconnected or blocked at the firewall from any external network during the installation of an operating system. Systems in a test and development enclave are not connected to the network until security controls as required by the appropriate STIGs are configured and validated by the IAO.

It is the responsibility of the IAO to ensure that all systems supporting application development, software testing, and operating system maintenance are connected to network enclaves isolated from production systems. At a minimum, these systems must be on a separate network segment with access controls restricting use to only the networks required to support the specific customer or operational requirements. If access to the development or testing systems must be accomplished from outside the development enclave, out-of-band access must be utilized. Out-of-band access is discussed in-depth in the *Network Infrastructure STIG*.
Additional requirements for a Test and Development enclave will be provided in an update to this document.

- *(ENTD100: CAT II) The IAO will ensure all systems supporting application development, software testing, and OS maintenance are connected to an isolated network separated from production systems.*

- *(ENTD110: CAT II) The IAO will ensure out-of-band access is utilized if outside access to the test and development systems is required.*

2. ENCLAVE SECURITY GUIDANCE

There are numerous security requirements that have been established for DOD information systems and networks to secure the enclave boundary and the information systems that reside within. In this document, an enclave boundary is an entry/exit point of a network of dissimilar security policy (i.e., it is not referring to different classification level domains). Enclave security should begin with a clear and concise security policy for each enclave. Knowing what the risks are to the environment is a key factor in determining what security controls are needed to eliminate or reduce this risk. The following sub-sections outline initial requirements for all DOD computing environments to include the National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP 11) Policy, MAC, and traditional and physical security.

2.1 Information Operations Condition (INFOCON)

Additional considerations and requirements are currently being addressed due to varying levels of INFOCON conditions in different theatres of operation. Guidance on the changing requirements will be forthcoming. As of this writing, the current INFOCON guidance has not yet been rescinded.

The INFOCON for the DOD recommends actions to uniformly heighten or reduce defensive posture, to defend against computer network attacks, and to mitigate sustained damage to DOD information infrastructure, including computer and telecommunications networks and systems. It is the responsibility of the site to ensure compliance with the Chairman Joint Chiefs of Staff (CJCS) INFOCON Memo that was signed on 10 March 1999 by General Joseph W. Ralston, Acting Chairman of the Joint Chiefs of Staff. Additionally, the IAM will be responsible for developing any new supplemental procedures that are required (or for modifying old procedures) in order to comply with INFOCON guidance.

2.1.1 Description

The INFOCON system presents a comprehensive, structured, coordinated approach to react to and defend against attacks on DOD computers and telecommunications. The INFOCON system impacts all personnel who use DOD information systems, protects systems while supporting mission accomplishment, and provides an overall defensive effort through adherence to standards. While all communications systems are vulnerable to some degree, factors such as low-cost, readily available information technology, increased system connectivity, and standoff capability make a computer network attack (CNA) an attractive option to DOD adversaries at present. CNA is defined as "*operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.*" INFOCON also outlines countermeasures to prevent scanning, probing, and other suspicious activity, unauthorized access, and data browsing. INFOCON levels are NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA.

2.1.2 Authority

The INFOCON system was established by the Secretary of Defense and administered through the Director of Operations, Joint Staff (J-3). INFOCON applies to the Joint Staff, Combatant Commands, and Defense Agencies, as well as joint, combined, and other DOD activities throughout the entire conflict spectrum—peacetime through war. In addition to the CJCS CM-510-99, the DISA CIO Memorandum, 15 November 2002, INFOCON Interim Guidance provides additional guidance to DISA networks.

2.1.3 INFOCON Levels

Normal - Normal Activity
- o No Significant Activity

Alpha - Increased Risk of Attack
- o Indications and Warnings (I&W) indicate a general threat.
- o Regional events occurring which affect US interests and involve potential adversaries with suspected or known CNA capability.
- o Military operation, contingency or exercise planned or ongoing requiring increased security of information systems.
- o Information system probes; scans or other activities detected indicating a pattern of surveillance.

Bravo - Specific Risk of Attack
- o I&W indicate targeting of specific system, location, unit, or operation.
- o Major military operation or contingency, planned or ongoing.
- o Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance.
- o Network penetration or denial-of-service attempted with no impact to DOD operations.

Charlie - Limited Attacks
- o Intelligence attack assessment(s) indicate a limited attack.
- o Information system attack(s) detected with limited impact to DOD operations:
- o Minimal success, successfully counteracted.
- o Little or no data or systems compromised.
- o Unit able to accomplish mission.

Delta - General Attacks
- o Successful information system attack(s) detected which impact DOD operations.
- o Widespread incidents that undermine ability to function effectively.
- o Significant risk of mission failure

- *(EN050: CAT III) The IAO will ensure compliance with INFOCON procedures in accordance with the CJSC INFOCON Memo, dated 10 March 1999.*

- *(EN070: CAT III) The IAO will develop and maintain supplemental procedures for use by the SAs as required, in consonance with INFOCON guidance.*

2.2 National Information Assurance Partnership (NIAP) and NSTISSP 11

The NIAP is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers. NIAP is the collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). NSTISSP 11, states that all IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DOD information systems must be evaluated and validated in accordance with the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, or the NIST Federal Information Processing Standard (FIPS) validation program. Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase.

At the enterprise level, implementation-independent specifications for IA and IA-enabled IT products are provided in the form of protection profiles. Protection profiles are developed in accordance with the CC within the NIAP framework. The CC is an international effort to standardize and improve existing evaluation criteria. Regardless of the mission assurance category or confidentiality level of the DOD information system, all incorporated IA products, and IA-enabled IT products that require use of the product's IA capabilities, acquired under contracts executed after 1 July 2002, shall comply with the evaluation and validation requirements of NSTISSP No. 11.

Evaluation Assurance Levels (EALs) are predefined assurance packages selected by the authors of the Common Criteria to represent points on the CC assurance scale. These predefined levels go from EAL1, the lowest level of assurance, to EAL 7, which is the highest. In general, the U.S. DOD views EALs 1 and 2 as Basic Level Assurance, Levels 3 and 4 as Medium Level Assurance and Levels 5 through 7 as High Level Assurance. Reliance on EALs alone does not provide a method for determining the "security robustness" of a product. The EAL merely provides a convenient reference for the amount of analysis and testing performed on the product. Users are encouraged to read both the security functionalities as well as the EAL specified in the security target to determine whether the "security robustness" of the product is appropriate for their environment.

COMMON CRITERIA	*US TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC)*	*TESTING CRITERIA*
EAL1		Functionally tested
EAL2	C1 Discretionary Security Protection	Structurally tested
EAL3	C2: Controlled Access Protection	Methodically tested and checked
EAL4	B1: Labeled Security Protection	Methodically designed, tested and reviewed
EAL5	B2: Structured Protection	Semi-formally designed and tested
EAL6	B3: Security Domains	Semi-formally verified design and tested
EAL7	A1: Verified Design	Formally verified design and tested

Table 2-1. Evaluated Assurance Levels

Robustness describes the strength of mechanism (e.g., the strength of a cryptographic algorithm) and assurance properties (i.e., confidence measures taken to ensure proper mechanism implementation) for an IA solution. The more robust a particular component is, the greater the level of confidence in the protection provided to the security services it supports.

It is also possible to use non-technical measures to achieve the equivalent of a level of robustness. For example, physical isolation and protection of a network can be used to provide confidentiality. In these cases, the technical solution requirement may be reduced or eliminated.

Additional information on Common Criteria, a listing of validated products or products in evaluation, as well as protection profiles may be obtained from http://niap.nist.gov. Refer to DODI 8500.2 for DOD acquisition and protection profile requirements.

- *(EN080: CAT III) The IAO will ensure all IA or IA enabled products purchased after 1 July 2002 meet the minimum EAL and robustness level requirements as established by the Designated Approving Authority (DAA).*

- *(EN090: CAT III) The IAO will ensure the acquisition of IA or IA-enabled products meet the requirements as set forth by NSTISSP 11 and the DODI 8500.2.*

2.3 MAC

MAC are based on the mission needs of the warfighter and used primarily to determine requirements for information systems integrity and availability. A MAC is always teamed with an independent level of confidentiality. Enclaves always assume the highest mission assurance category and security classification of the applications or IT-based processes they support, and derive their security needs from those systems (DOD 8500.2.) The three levels of confidentiality are High – processing of Classified information; Medium – processing sensitive information; and Basic – processing public information. The DOD has defined three Mission Assurance Categories:

- MAC I: Require the most stringent protection measures. MAC I systems require high integrity and high availability for information systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

- MAC II: Require additional safeguards beyond best practices to ensure adequate assurance. MAC II systems require high integrity and medium availability for information systems handling information that is important to the support of deployed and contingency forces.

- MAC III: Require protective measures, techniques, or procedures generally commensurate with commercial best practices. MAC III systems require basic integrity and basic availability for information systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term.

- *(EN100: CAT III) The IAM will ensure all DOD information systems and enclaves are assigned a mission category directly associated with the importance of the information they contain relative to the achievement of DOD goals and objectives, particularly the warfighter's combat mission. (DODI 8500.2)*

2.4 System Connection Approval

The DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Instruction is the standard DOD process for identifying information security requirements, providing security solutions, and managing information system security activities. The DITSCAP formalizes the C&A process. Procedures outlined in the DITSCAP explain the process that provides discipline as the Enclave Security and Architecture are applied to specific requirements. The System Security Authorization Agreement (SSAA), which is a formal agreement and baseline security configuration document, is used throughout the entire DITSCAP process to guide actions, document decisions, specify security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security. Each SSAA will include a description of the architectural implementation of the security requirements identified in this STIG. The objective is to use the SSAA to establish a binding agreement on the level of security required before the system development begins or changes to a system are made.

Combatant Commands, Services, and Agencies have a responsibility to protect DOD worldwide networks in support of the warfighter. To properly execute this task, all entities have a personal obligation and responsibility to ensure their internal networks are protected as well. The DITSCAP, STIGs, CAPs, IAVM Notices, INFOCON, certification of personnel (i.e., SAs and end users), and other DOD initiatives have been implemented to assist and guide the Department in managing its information technology security risks. Individually each initiative has proven valuable and useful. The purpose of the IA enclave concept is to bring these individual security elements together, or provide an umbrella for them, to form a stronger, more robust entity that will provide a higher level of assurance. The IA enclave concept should provide for quicker reaction time and positive control during cyber attacks or disruptions.

To implement the enclave concept will require the baselining of current internal networks to identify each individual enclave that when aggregated together compose the entire internal networking environment. Once every enclave is identified, each will have a manager assigned who will be accountable for ensuring all connection approvals, STIGs, IAVM Notices, INFOCONs, etc., are implemented for all components of their enclave, in essence an enclave connection approval process. It is the responsibility of the Combatant Commands, Services, and Agencies to create internal connection and approval requirements.

The goal of each enclave is to attain an acceptable level of compliance and to maintain that level to earn and retain a certificate of "networthiness." A certificate of "networthiness" will be earned by successfully completing certification actions through self-assessment and third-party checks. The appropriate accreditor will issue each certificate.

2.5 Traditional Security

Traditional Security, as part of enclave security, requires a thorough evaluation of individuals who control, operate, design, and/or manipulate networks and or data to ensure their trustworthiness, loyalty, and reliability. It also incorporates physical security protective measures using the Defense-in-Depth philosophy. These measures include a security program consisting of layered and complementary security controls, approval and certification of controlled areas, perimeter barriers, random guard patrols, and closed circuit video that are sufficient to deter, detect, respond, and neutralize any threat and/or unauthorized entry and movement within a facility. Physical security mechanisms include elements such as site design and layout, fire and power protection, training, and emergency response procedures. Physical security controls include physical access, technical, environmental and life safety, and administrative controls. All of these controls are identified in numerous DOD Directives and Instructions (e.g., DOD 5200.1-R Information Security Program Regulation, 17 January 1997).

2.5.1 Training

Security awareness programs provide basic information and the understanding of the importance of security. Formal security training and education programs provide in-depth knowledge of specific security threats and mitigation of those threats. Requirements for formal and awareness training are outlined in the DODD 8500.1, and the CJCSI 6510.01-C Information Assurance and Computer Network Defense, May 2001.

- *(EN110: CAT II) The IAM will ensure the DOD component develops and implements security training and certification plans and procedures for all personnel who use DOD computer systems or perform the duties of a System Administrator.*

- *(EN120: CAT III) The IAM/IAO will establish and implement a comprehensive user security features training program to include password and Internet usage guidance.*

- *(EN130: CAT II) The IAM will provide training and certification for all privileged users (i.e., SAs and network administrators), as well as for all IAOs and other professional or management security personnel based on DOD standards for certification.*

2.5.2 Authorization and Access

In order to ensure the confidentiality of an IS, a determination needs to be made as to whether a user has the appropriate credentials to access a system or network. The need-to-know principle is determined by the necessity for access to, knowledge or possession of, specific official DOD information required to carry out official duties. The need-to-know determination is derived from a decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties. Need-to-know principles are applied to ISs within the DOD, and appropriate measures must be in place in order to verify and authorize individuals at all levels. This can be accomplished using various methods such as denying access after multiple unsuccessful logon attempts; however, stringent controls must be in place to standardize this process. Strong authentication controls such as PKI should be used for all privileged access.

- *(EN140: CAT II) The IAM will ensure that privileged users and IAOs access only that data, control information, software, and hardware for which they are authorized access and have a need-to-know.*

- *(EN150: CAT II) The IAM/IAO will ensure users have a validated or demonstrated need-to-know to access information, and discretionary or role-based access controls will be established and enforced, via operating system controls and access authorization forms, by the Information Owner.*

- *(EN160: CAT II) The IAM/IAO will ensure all individuals with access to a DOD system or network require the following in the form of a DD Form 2875 or similar access authentication form:*

  - *Verification of the user's security clearance and/or investigative requirement for holding an IT (formerly ADP) position.*

  - *Verification of the need-to-know and permission to access the data by the information owner.*

  - *Verification of training.*

  - *Acknowledgment, in writing, of the user's responsibilities to protect the system, data, and password.*

- *(EN0170: CAT II) The IAM/IAO will ensure personnel authorization and investigation requirements are processed in accordance with DODI 8500.2.*

2.5.3 Physical Security

Physical Security is concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, facilities, material, and data; and to safeguard them against espionage, sabotage, damage, and theft. Lighting, fire suppression, humidity controls, locks, guards, etc., all contribute to the security of DOD information systems and the missions they support.

- *(EN180: CAT II) The IAO will ensure only authorized personnel with appropriate clearances are granted physical access to DOD computing facilities.*

- *(EN190: CAT III) The IAO will ensure all physical and environmental controls are established in accordance with DODI 8500.2, DOD 5200.1-R Information Security Program, and the 5200.2-R Personnel Security Program.*

- *(EN200: CAT II) The IAO will ensure procedures are in place for the removal or destruction of data by clearing, sanitizing, or destroying of classified media or equipment, prior to release outside of the security domain.*

2.5.4 Backup and Recovery

Backup and recovery procedures are critical to IA and the protection of the infrastructure. If a system is compromised, shut down, or otherwise not available for service, this could hinder the availability of resources to the warfighter.

- *(EN210: CAT II) The IAM will ensure the continuity of operations (COOP) or disaster recovery plans or significant portions are exercised in accordance with the MAC level.*

- *(EN220: CAT II) The IAM will ensure a disaster plan exists that provides for the resumption of mission or business essential functions within the specified period of time depending on MAC level. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)*

- *(EN230: CAT II) The IAO will ensure all critical systems, to include infrastructure devices such as routers and inventory records, are backed up and copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational equipment or software.*

- *(EN240: CAT II) The IAO will ensure data backup is performed daily, and recovery media is stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.*

NOTE: On-line backups to remote sites meet the requirement for off-site storage; however, off-line backups are also required to ensure integrity of the data.

2.6 Patch Management

Due to viruses, worms, Trojans, and other malicious software, in addition to inevitable weaknesses in code, the necessity to patch critical vulnerabilities is paramount. As part of the general practice of performing system administration, it is imperative that SAs monitor security vulnerabilities from the vendor of their particular system.

- *(EN040: CAT II) The IAO will ensure all security-related patches are applied.*

- *(EN041: CAT II) The IAM will ensure there is a documented security patch management process, to include procedures, in place. The patch management process will ensure all security related patches are applied and that the process can be validated.*

- *(EN042: CAT III) The IAM will ensure workstations take advantage of technology and use an automated patch distribution process from a trusted site or secure source (i.e., tools such as Software Update Services (SUS), scripts, Tivoli, etc.) to distribute and apply security related patches.*

- *(EN043: CAT III) The IAM will ensure testing of security patches is performed in a development or test environment (non-production environment) prior to deployment to production systems.*

The DOD Patch Repository can be accessed from the following URL:

https://patches.csd.disa.mil for NIPRNet

For additional information on the DOD Patch Repository contact Patch-Support@mont.disa.mil.

2.7 Enclave Perimeter Security

Enclave perimeter security mechanisms are employed at the boundary between a DOD controlled LAN and a WAN (e.g., LAN/NIPRNet backbone, LAN/SIPRNet backbone). These connections are discussed in this document as "LAN to WAN" connections.

Enclave protection mechanisms are also used to provide security for specific security domains. In general, enclave protection mechanisms are installed as part of an Intranet used to connect networks that have similar security requirements and have a common security domain. A large, complex site, such as a Data Center, may have multiple security domains with protection mechanisms tailored to the security requirements of specific customers. For example, Defense Finance and Accounting Service (DFAS) and Defense Logistics Agency (DLA) may have functionally driven security domains. There might also be technology-driven security domains for Multiple Virtual Storage (MVS), or vendor specific domains for Unisys, Tandem, etc. Smaller locations may have a single enclave with a single security domain supporting the entire organization. The enclave or system owner will identify security domain requirements in the SSAA.

STIGs, SRRs, and the DOD Ports, Protocols, and Services (PPS) Assurance Category Assignments List (CAL) provide the specifications, standards, and inspections for each of the key enclave components.

2.7.1 DOD Ports, Protocols, and Services (PPS) Assurance Category Assignments List (CAL)

The ASD-C3I, in coordination with the Defense-Wide Information Assurance Program (DIAP), the Joint Staff, USSTRATCOM, and DISA announced the DOD Ports and Protocols Program (PNP) with the release of the 28 January 2003 memorandum entitled "DOD Ports, Protocols, and Services – Increasing Security at the Internet/DISN Boundary." This program represents a fundamental change in the DOD Computer Network Defense (CND) philosophy, replacing the current CND philosophy of "Deny-by-exception" with "Deny-by-Default." Any PPS that is not specifically addressed will have a policy of "Deny." These concepts are incorporated in the DOD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM).

The program is an attempt to minimize the risk to DOD ISs by regulating access between the Internet and defense networks by implementing positive technical controls. By initiating and advocating standard configurations for ports, protocols, and services at the perimeter, DID may be improved along with the security posture and interoperability of the NIPRNet.

The program implements the blocking of service requests from the Internet to the DISN Unclassified IP routing networks, yet does not affect outbound connection requests to the Internet or internal DOD network traffic. DOD policy states that the guidance is optional for "nested" or otherwise contained within DOD component enclaves that do not provide boundary protection at DOD network boundary;" however, as is best practice and strongly recommended by the DOD 8551.1, LAN and WAN enclaves will adhere to this guidance.

The guidance does not address PPS within Virtual Private Networks (VPNs); therefore authorities operating VPNs will be responsible for the use of PPSs within their VPNs, and for security controls over VPN data content. As this may increase risk and jeopardize other enclaves, any decision to allow Red or risky traffic through a VPN must address the risk to other enclaves and must be approved by the DAA at each connecting site. When the VPN connects enclaves owned by more than one DAA, each must approve the connection.

The technical guidance lists three levels of blocking requirements at the enclave perimeter:

- Red Ports: Deny. No acceptable mitigation strategy and unacceptably high risk for routine use.

- Yellow: Deny/Conditional/Allow. May have associated risk that can be mitigated to an acceptable level. Yellow is not acceptable under all conditions, but rather can be brought to an acceptable risk level if required mitigation strategy is implemented and approved by the DAA.

- Green: Deny/Conditional/Allow. May have associated risk that can be mitigated to an acceptable level and considered best security practice and advocated for use in future applications.

- *(EN250: CAT II) The IAO will ensure the site has blocked all PPSs at the enclave perimeter in accordance with the DOD Ports, Protocols, and Services Assurance Category Assignments List and the Network Infrastructure STIG.*

- *(EN260: CAT I) In accordance with the DOD philosophy of permit by exception, the NSO will ensure router ACLs or firewall rules are based on a policy of Deny-by-Default with blocks on all services and protocols not required by the site. Either a firewall or router with deny-by-default ACLs must protect the Enclave perimeter.*

- *(EN270: CAT II) The IAO will ensure allowing Red traffic through a VPN addresses the risk to other enclaves and must be approved by the DAA.*

Reference the *Network Infrastructure STIG* to obtain additional configuration guidance for required PPS blocking at the enclave perimeter. See the following web site for additional details on the DOD Ports and Protocols Program: https://iase.disa.mil.

2.7.2 Minimum Enclave Requirements

In order to comply with the enclave architecture as it pertains to LAN/WAN enclaves, the minimum requirements include the following devices or systems:

- External Network Intrusion Detection System (IDS), anomaly detection, or prevention device if required by the Computer Network Defense Service Provider (CNDSP)
- Perimeter Protection
    - Router Security with Access Control Lists
    - Firewall and application level proxies. (May be separate device to proxy applications.)
- Internal Network Intrusion Detection (NID) system
- DMZ, if applicable for publicly accessible services
- Split Domain Name Service (DNS) architecture
- Secure devices and operating systems (i.e., STIG compliant)

- *(EN280: CAT III) The DSAWG, DAA, or SIPRNet Program Office will approve any exception to these requirements.*

Enclave Perimeter Security mechanisms for the LAN/WAN enclave are described in the following sections.

2.7.2.1 External Enclave Perimeter Intrusion Detection System

The external network intrusion detection system (NIDS) is a suite of software tools that support the detection, analysis, and gathering of evidence of intrusive behavior occurring on Ethernet or Fiber Distributed Data Interface (FDDI) based networks using IP.

A network intrusion detection system (NIDS) is one of the first layers of defense in the DID architecture. A NID allows for detecting, analyzing, and collecting intrusive behavior occurring on networks using the Internet Protocol (IP). The NIDS is passive, so intruders are not aware of its presence. Data can be analyzed real-time or collected for retrospective analysis. Alarms are generated based on event rules.

If the organization's CNDSP has determined that IDS data from this site significantly contributes to the global security picture, an external NIDS must be installed and implemented in front of the premise or border router. This traffic must be monitored by a certified CNDSP. DODD O-8530.1 requires all DOD components to establish or provide for a CND Service (CNDS).

The external NID provides four common operating models:

- Retrospective intrusion analysis
- Real-time intrusion detection
- Evidence gathering
- Statistics gathering

- *(EN290: CAT II) The IAM will ensure if directed by their CNDSP, the site will install and maintain an external NID at their enclave perimeter.*

- *(EN300: CAT II) The enclave perimeter NID will be under the operational control and configuration management of the appropriate CNDSP. Whenever possible, the enclave NID will be positioned outside of any local firewalls so that the CNDSP has visibility of all attempted malicious activity.*

- *(EN310: CAT III) The GNC will review and approve requirements for enclave perimeter Joint Intrusion Detection System (JID) to ensure integration with the Sensor Grid.*

Refer to the *Network Infrastructure STIG* for additional configuration requirements and guidance on external NID or JID systems.

2.7.2.2 Router Security with Access Control Lists

Routers support a large number of network services at various layers of the Open System Interconnection (OSI) model. Some of these services can be restricted or disabled, thus improving security without degrading the operational use of the router. Some of these services are application layer protocols that allow users and host processes to connect to the router. Others are automatic processes and settings intended to support legacy or specialized configurations but which are detrimental to network security. The best security practice for routers is to only support the services and protocols needed by the network to meet operational commitments.

Routers also support Access Control Lists (ACLs), which provide a basic level of access control over network connections based on the site's local security guidance. These controls include restrictions on inbound and outbound connections, as well as on connections between LAN segments internal to the site/enclave. These restrictions are based on the source and destination addresses of the IP packet as well as the service type (e.g., Simple Mail Transfer Protocol [SMTP], e-mail, Telnet, and Hypertext Transfer Protocol [http]).

- *(EN320: CAT II) The NSO will ensure routers are configured in accordance with the Network Infrastructure STIG.*

- *(EN330: CAT II) The NSO will ensure egress filtering rules are applied denying all outbound traffic with illegitimate (i.e., not local network) IP addresses and both ingress and egress filtering rules are applied denying all Distributed Denial of Service (DDOS) ports and IPs in accordance with the Network Infrastructure STIG.*

The Enclave Management Control Board (EMCB), SIPRNet Program office, or appropriate DAA will address any exceptions to these requirements through the Enclave Security Extension process.

Refer to the *Network Infrastructure STIG* and the DOD PPS Assurance Category Assignments List (CAL) for additional information on PPS and configuration requirements.

2.7.2.3 Enclave Firewall

Firewalls are one aspect of a DID security strategy. A firewall is one or more computer systems or devices that enforce an access control policy between two networks. Firewalls control the traffic flow between a trusted network and an untrusted network. The *Network Infrastructure STIG*, along with the CJCSM 6510.01, outline firewall implementation requirements, modern Commercial-Off-The-Shelf (COTS) firewall functions, the firewall implementation reporting and extension process, required filtering rules, and guidance for developing firewall compatible applications.

There are four basic classifications of firewalls, which are packet filtering, circuit-level gateway, stateful inspection, and application-level gateway. Packet filtering firewalls permit or deny traffic based solely on the headers of the individual packets. It examines the packets both inbound and outbound, source and destination UDP/TCP port, and source and destination IP addresses. A packet filtering firewall is inexpensive and fast, yet does not support strong user authentication and has no protection from IP or DNS address spoofing. A circuit-level gateway completes a connection between a client and server without interpreting the application protocol. If a permitted connection is established, a virtual circuit is created for the session allowing packets to flow to the hosts without additional inspection. Easy maintenance and wide range of protocol support are advantages to a circuit-level gateway; however, limited logging capability and dependence on the trustworthiness of the hosts are serious disadvantages to this firewall type. A stateful inspection firewall looks at the same headers as packet filters. More importantly, this technology allows the firewall to dynamically maintain state and context information about past packets. Security decisions can then be based on this state information.

An application-level gateway is generally considered to be more secure than other firewall types, in that the proxy implementation does not allow for direct communication between hosts and it can be used to implement strong user authentication in applications.

Proxy services are required to isolate the inside environment from the outside environment while still maintaining an information source for users inside the enclave. Web proxy services will be provided as a minimum. Although network performance may be affected by the implementation of an application level gateway, in order to support DID, an application level gateway is recommended at the enclave perimeter. Due to technological advances there are devices such as SSL Gateways, E-mail Gateways, etc., that will proxy services to protect the enclave. Therefore, a layer 4 or stateful inspection firewall, in collaboration with proxy devices to service all connections, is an acceptable alternative.

The *Network Infrastructure STIG* prescribes the policy for current and planned firewalls and is intended to facilitate the effective and uniform implementation of firewalls across DOD organizations. The *Network Infrastructure STIG* details the requirements for placement, which can vary due to the sensitivity of the networks, the network infrastructure, and the type of network traffic. Usually firewalls are used to protect the boundaries of a network, although, at times, they can be used to secure a sensitive part of an enclave from the rest of the enclave. There are three main points at which a firewall can be implemented within a network:

- At LAN-to-WAN/WAN-to-LAN connections
- At LAN-to-LAN connections
- At WAN-to-WAN connections

LANs and enclaves can be classified as Top Secret, Secret, Controlled Unclassified Information (CUI), and Unclassified. WANs also have different classification requirements such as Joint Worldwide Intelligence Communications System (JWICS), Secure Internet Protocol Router Network (SIPRNet), Unclassified Internet Protocol Router Network (NIPRNet), and public or Internet. An example of a LAN-to-WAN connection could be an unclassified enclave with a connection to the Internet. A LAN-to-LAN connection could consist of a security domain interconnecting to another security domain LAN within the same enclave to allow separation from other groups and information sharing between the two. Both of these connections are boundaries where a firewall is required to ensure the confidentiality, availability, and integrity of the resources within that boundary.

Firewall Administrators (FAs) have the ultimate responsibility of ensuring that the firewall is configured and maintained in accordance with the requirements set forth by the DOD. FAs are responsible for the following:

- Seeking training to improve their knowledge and skills in the areas of network technologies, firewall configurations, and IA

- Assessing the security posture (configuration) of the firewall on a random basis using recommended tools and manual procedures

- Monitoring the firewall for penetration attempts or attempts to evade security

Auditing is a critical component of firewalls. The firewall provides an ideal place to log all of the traffic and activity on the network. Most firewalls log the time, type of service, and source and destination ports of incoming packets. Some firewalls allow the selection of certain events to be logged. Firewalls can provide for automatic notification of the administrator via pager or e-mail, depending on the type of access attempts. In some cases, the firewall can then attempt to trace future attempts at access to gain more information about the attacker. When subjected to various DoS attacks, some firewalls can either deny packets to guard against the attack or shut down entirely. Due care should be taken when shutting down traffic in order to avoid a self-imposed denial of service. One of the most difficult aspects of a network or firewall administrators duties is to verify and validate that the traffic passing through the firewall is legitimate. Firewall logs can contribute to this effort, yet an aggregation of the information collected from many sources (such as firewalls, IDSs, server logs, audit servers, etc.) would be most useful in determining whether or not an activity taking place is an attack on the infrastructure. Many vendors now see the need to incorporate such a facility into their products, as administrators do not have sufficient time to devote to reviewing audit and log files.

- *(EN340: CAT I) The NSO will ensure enclave firewalls are configured with the most restrictive security rules possible ("that which is not expressly allowed is denied") (Deny by Default). A Firewall Implementation Description Report are developed and maintained for each managed firewall. The organization's SSAA is updated to reflect the firewall installation or modification for the system using the firewall. Appropriate references between documents are encouraged to reduce redundancy.*

- *(EN350: CAT II) The IAO will ensure only COTS firewall products that meet the criteria set forth in the Network Infrastructure STIG and the CJCSM 6510.01 are employed.*

- *(EN360: CAT III) The IAO will ensure all permitted IPs and PPSs are documented.*

- *(EN370: CAT I) The IAO will ensure direct network connections between managed networks and the Internet, NIPRNet, SIPRNet, or other external networks do not exist if there is no DOD approved waiver for the connection.*

Refer to the *Network Infrastructure STIG* for additional information and configuration requirements.

2.7.2.4 Virtual Private Network (VPN) Encryption

VPNs provide a variety of methods to protect network data integrity, confidentiality, and availability using techniques such as connectionless integrity, data origin authentication, traffic analysis, and access protection. A VPN is a private data network that maintains confidentiality by using encryption and security procedures across a shared public telecommunications infrastructure. The data is transported or tunneled across a public or private network employing encryption technologies such as Layer 2 Tunneling Protocol (L2TP), Point-to Point Tunneling Protocol (PPTP), and Internet Protocol Security (IPSec). Typically, VPN encryption is implemented at the local network entry point (i.e., the firewall or Premise router), thereby freeing

the end systems from having to provide the necessary encryption or communications security functions.

PPTP, an extension of the Internet's Point-to-Point Protocol (PPP), allows a host with PPP client support to use an Internet Service Provider (ISP) to connect securely to a server elsewhere in the local area network. L2TP is an extension of PPTP, which enables VPN implementation by merging PPTP and Layer 2 Forwarding (L2F) protocols. L2TP does not include mechanisms for encryption or authentication and must obtain these services in conjunction with other devices or protocols.

IPSec is the most widely used secure network protocol. IPSec provides VPN capabilities at Layer 3 of the OSI model, whereas PPTP and L2TP operate at Layer 2. IPSec consists of two packet encapsulation protocols—the Authentication Header (AH) that allows authentication of the sender; and the Encapsulating Security Payload (ESP) that supports both authentication of the sender and encryption of data. In addition, IPSec supports two encryption modes—transport and tunnel. Transport mode encrypts the data portion (payload) of each packet, but does not encrypt the header. Tunnel mode encrypts both the header and the payload, making this mode more secure. In either mode, the receiving side of an IPSec compliant device decrypts each packet.

VPNs can be divided into three categories—remote access, site-to-site, and extranet. The type of VPN technology employed is based on bandwidth requirements, resources, and differing security needs, all of which is determined by the function it will perform and impacts the placement of the device in the network infrastructure. Placement of the VPN should not adversely impact the enclave security and all VPN traffic must pass through the Enclave Security Architecture. Although encrypted data (e.g., Secure Socket Layer [SSL], Secure Shell [SSH], Transport Layer Security [TLS]) that enters the VPN tunnel does not need to be unencrypted prior to leaving the tunnel, the data must pass through the respective application proxy on the firewall. Host-to-gateway VPNs are preferred; however, if a host-to-host VPN is required to meet mission needs, it will be established between trusted, known hosts. (Refer to the *Network Infrastructure STIG*.)

Commercial VPN mechanisms may be used for encryption of unclassified and classified data that will be handled at its original level (e.g., for privacy of secret data across the SIPRNet). Activities that communicate via VPNs are responsible for identifying and agreeing to all external connections for each managed network, agreeing to the policies enforced by firewalls on each managed network, and accepting the residual risks of each managed network connected by the VPN.

- *(EN390: CAT II) The NSO will ensure all VPN implementations adhere to the VPN section of the Network Infrastructure STIG.*

- *(EN400: CAT II) The NSO will ensure VPNs are established as tunnel type VPNs that terminate outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router). Location is not as paramount as being in compliance with DODI 8500.2 EBVC-1 "VPN traffic is visible to network IDS."*

- *(EN410: CAT II) The NSO will ensure all VPN communications to/from the network employ at a minimum a FIPS 140-2 approved data encryption algorithm (i.e., Advanced Encryption Standard (AES) or Triple-Data Encryption Standard [3DES]). (See http://csrc.nist.gov/cryptval.)*

- *(EN420: CAT II) The NSO will ensure that at a minimum, all VPN solutions include an IDS capability on the unencrypted portion of the network or system. DODI 8500.2 IA Control EBVC-1 requires that all VPN traffic is visible to a Network IDS.*

Refer to the *Network Infrastructure STIG* for additional VPN information, placement, and configuration requirements.

2.7.2.5 Domain Name Service (DNS)

DNS is an essential capability within the DOD network infrastructure that provides the translation between host names and IP addresses. Because DNS is such an essential capability, it represents a significant potential target of opportunity for cyber-attacks.

The DNS is a hierarchically structured, distributed database system used to map host names to IP addresses, and vice versa. The DNS is designed with implicit trust in its peers and in the packets received. In its normal mode of operation, hosts send queries to DNS servers who reply with either the proper answer or with a pointer to a smarter DNS server. DNS sub-hierarchies can be delegated to other servers for ease of operation.

As hosts are added, removed, or modified, the controlling organizations for the respective domains, such as that for .mil, provide an update to the DNS database. The update is replicated throughout the DNS architecture until every name server has the update, or at a minimum, knows where to find it. DoS, cache poisoning, and spoofing are just a few of the attacks that have been launched against a DNS server. These attacks, if successful, can disrupt an entire network. In order to mitigate the risk to the DNS structure, split DNS, securing the DNS server, and using the appropriate DNS application are imperative.

- *(EN430: CAT II) The IAO will ensure that the DNS server and architecture are configured in accordance with the DNS STIG.*

Refer to the *DNS STIG* for additional information and configuration requirements.

2.7.2.6 Local Enclave Network IDS (NIDS)

The enclave Network IDS (NIDS) will monitor internal network traffic and provide real-time alarms for network-based attacks. Either the CNDSP or the local staff may control the enclave NIDS rules, policy rules, and attack signatures. The site may establish a support agreement with the CNDSP for monitoring. The local staff is responsible for initial response to real-time alarms. Significant incidents such as any attempt to deny, degrade, disrupt, obtain, or destroy data, are reported to the site's CNDSP. Extensions will be granted by the EMCB or DAA on a case-by-case basis.

Refer to the *Network Infrastructure STIG* for additional information and configuration requirements.

2.7.2.7 Privileged User Remote Access

All remote access to a DOD information system will be mediated through a managed access control point such as a Remote Access Server (RAS) or VPN device. These devices, used by SAs to remotely configure or monitor devices within an enclave, must be located in controlled areas for physical protection. According to the DODI 8500.2, IA Control EBRU-1, remote access will use encryption to protect the confidentiality of the session. IA Control EBRP-1 discourages the use of remote access by privileged users unless compelling operational need is documented.

For the purpose of this document, remote access for privileged users is defined as privileged remote users who will be connecting to a DOD core network to perform any system administration duties to include troubleshooting, configuration changes, and reviewing any system or configuration data, regardless of system type. This type of access will require the most stringent security controls; users must use government owned or controlled devices; will employ encryption; and an audit trail of each remote session will be recorded and reviewed. As privileged users, SAs perform duties such as configuration changes, troubleshooting application and communications issues, and logging on to a system with privileges to perform maintenance functions; therefore, rigorous security measures must be in place to protect the data and communication to and from the system. Privileged user access will require the use of encryption on all communication channels between the remote user and the system being accessed. If the system requires the use of a clear-text based terminal emulator such as TN3270 (which accesses 3270 and 5250 based applications over TCP/IP) or Telnet, the only acceptable methods of connectivity will be an encrypted session, the employment of VPNs, Secure Web Access (SWA) with SSL, TLS, IPSEC, or SSH. Encryption on an unclassified network should be used to protect the End-User access level. However, as of this writing, it is not required, but rather it is a strongly suggested practice. In the Classified arena, however, Type 1 encryption is a requirement for all access. VPN traffic is allowable on top of Type 1 encryption on the SIPRNet; however, Type 1 encryption is the foremost requirement.

- *(EN440: CAT I) The IAO will ensure all privileged user access to a DOD system or resource is secured using an acceptable form of encryption to secure the data traversing the network. This applies to unclassified data only. Classified data requires Type I encryption.*

- *(EN450: CAT II) The NSO will ensure remote access device traffic/data does not bypass the security architecture as outlined in the Network Infrastructure STIG (i.e., all ingress traffic passes through the firewall and NIDS).*

Refer to the *Network Infrastructure STIG*, and the *Desktop Application STIG* for additional guidance and configuration requirements for remote access.

2.7.2.8 Content Security Checking

Many forms of computer information can contain harmful content including viruses, macro viruses, Trojan Horse programs, worms, etc. This malicious software, often referred to as "malware," can be transmitted across a network in a number of ways including SMTP e-mail attachments, ftp file downloads, and Java applets. Incoming data can be checked for harmful content at the public network boundary. Numerous COTS products exist that can perform this type of content security checking. Email sweepers, anti-virus software and proxy devices can perform content security checking. Applications such as Norton Anti-Virus, McAfee Anti-Virus, and Trend Micro products are available on the DOD-wide virus detection tool site license. (See http://www.cert.mil/.) A complete list of approved attachment types can be found in NSA's *Outlook E-Mail Security in the Midst of Malicious Code Attacks*, which can be obtained at http://www.nsa.gov/snac/.

- *(EN460: CAT III) The IAO will ensure all networks employ Content Security Checking, mechanisms for e-mail with attachments, ftp data, and http data. Products from the DOD standard anti-virus contract should be used.*

- *(EN470: CAT I) The IAO will ensure updated virus detection signatures are downloaded and installed, at least every 14 days or when the CERT provides an update.*

2.8 Demilitarized Zone (DMZ) or Service Network

A DMZ or Service Network provides enhanced security for servers that provide data to users outside of an enclave. The DMZ is a perimeter network segment that enforces the internal networks information assurance policy for external information exchange. DODI 8500.1, IA Control EBPW-1, states that connections between DOD enclaves and the Internet or other public or commercial WANs require a DMZ. Therefore, a DMZ will be established within the enclave Security Architecture to host any publicly accessible systems (e.g., ftp servers, public web servers, mail servers, external DNS, X.500 directories, etc.). Although there are many schools of thought and different architectural approaches, at a minimum, the DMZ will be established on a separate network interface of the enclave perimeter firewall. Firewall architectures are further detailed in the *Network Infrastructure STIG* and the CJCSM 6510.01. All DMZ traffic will be routed through the firewall for application-level processing and the DMZ will be isolated from the rest of the protected network.

- *(EN480: CAT II) The IAO will ensure a DMZ is established within the Enclave Security Architecture to host any publicly accessible system.*

- *(EN490: CAT II) The IAO will ensure the DMZ is located on the network segment connecting the firewall to the border router or on a dedicated network segment connected to the firewall.*

Refer to the *Network Infrastructure STIG* for firewall placement and DMZ configuration information.

2.9 Port Security

As it is relatively easily to attach a network cable to notebook computers and small PCs and gain instant network access, controls need to be established to limit this type of network intrusion by unauthorized devices. There are numerous methods available from network device vendors to prohibit this unauthorized connection, yet some of these methods can be time consuming and a daunting task when there are many other issues facing the network administrator. Methods such as MAC address restrictions can be very valuable and secure; however it is rather easy to spoof a MAC address and this is a time intensive effort. There are devices that have the ability to turn off the network port when not in use; however this can be very difficult as users travel and are often in and out of the traditional worksite.

Due to technological advances there are now other alternatives to secure ports on the network in order to avoid unauthorized devices and or users from connection to the LAN. The IEEE 802.1X protocol allows LAN switch vendors the ability to implement port authentication and identification of users and devices. This implementation of the use of a protocol to secure network ports and to allow only those devices and users that have the appropriate credentials to obtain network connectivity, even prior to gaining access to network resources such as a servers, provides a more reliable way to secure Classified and other DOD sensitive networks.

- *EN865: CAT II) The IAO will ensure a port security solution is in place to protect access to the network.*

2.10 FTP and Telnet

Under certain circumstances the use of FTP and telnet may be the only viable solution (primarily due to legacy applications); however, the use of FTP and telnet is not a recommended best practice. The use of clear text transmission will be phased out as quickly as possible and the use of encrypted sessions will be implemented in the architecture. The use of an encrypted session and certificate-based authentication is required if supported by the device.

- *(EN870: CAT: II) The IAO will ensure if encryption protocols such as SSL or SSH transmit traffic directly to a host, a host based intrusion detection (HID) system is employed on the device if supported.*

- *(EN880: CAT: II) The IAO will ensure all network traffic is visible to an Intrusion Detection System (IDS). VPN traffic does not bypass the security architecture and must terminate in order for the traffic to be processed by a network IDS (NID) or Host Based IDS (HID).*

FTP and telnet are permissible inside an enclave, behind the premise router and protected by a firewall and router access control lists (ACLs); however, the requirement must be documented and maintained by the Information Assurance Officer (IAO). If either of these services is not required, the service will be deleted, disabled, or turned off. If the service is disabled or turned off, the site will continue to ensure that all appropriate patches are applied. When used, all associated traffic will be restricted by IP source and destination address if technically feasible, and other mitigating controls as required by the appropriate STIG will be enforced.

- *(EN890: CAT: I) The IAO will ensure FTP and telnet from outside the enclave into the enclave is not permitted, unless encrypted and the following conditions apply:*

  - *FTP and telnet are acceptable from outside the enclave through a remote access Virtual Private Network (VPN). The connection will terminate outside the firewall as to not bypass the security architecture. The connection will be proxied at the firewall or via an FTP/telnet proxy.*

  - *FTP and telnet are acceptable via a site-to-site VPN between trusted enclaves; however, an Acknowledgement of Risk letter (AORL) or documentation in the SSAA must already be in place for the tunnel. FTP and telnet are acceptable within distributed enclaves, if required, as long as the traffic is physically or logically segregated from normal traffic using a method supported by the network technology to create a virtual connection (e.g., VLAN, VPN, LANE, MPLS, IPSec tunnels).*

In addition to the data transmission being in the clear, the user credentials are also passed in the clear, which violates the DOD 8500.2, IA Control IAIA-1. As mitigation for this vulnerability, special consideration must be given to account maintenance and the types of user privileges associated with these accounts.

- *(EN900: CAT: II) The IAO will ensure all user FTP UID passwords have an expiration date and the password is changed every 90 days.*

- *(EN910: CAT: I) The IAO will ensure under no circumstances are FTP or telnet used with a userid (UID)/password that has administrative or root privileges.*

System-to-system FTP accounts (no user intervention) may be treated as an application-type account and the password will be changed at least once a year or when an administrator with knowledge of the password leaves. A system-to-system FTP account is defined as an account that a human never logs on to. It is only used for authentication of a process or batch job. If a single account is used both by a person and by a system for FTP or any other access, then the password for this account will need to expire every 90 days. Accounting must be configured to alert the system administrator of unauthorized access using system-to-system accounts or accounting logs must be reviewed on a weekly basis to detect unauthorized access. If unauthorized access using a system-to-system account is detected, immediate action will be taken to change the affected account password.

When FTP is used for system-to-system FTP, an acknowledgement of risk letter is required. A system-to-system transfer via a VPN would not require an acknowledgement of risk letter.

The acknowledgement of risk letter (AORL) or the SSAA will be used to document the use of unencrypted FTP or telnet or the risk will be accepted as part of the accreditation package (SSAA). The customer (data owner), the local DAA (when the site is not the data owner) will sign an acknowledgement of risk letter. The IAO will maintain the acknowledgement of risk. This acknowledgement of risk will identify the UIDs, passwords, and the data that is being transmitted unencrypted inside the site's enclave. The acknowledgement of risk will be dated and will be reviewed and renewed at least every 18 months.

An "anonymous" FTP connection within the enclave will not be allowed. Individual UIDs will be created for each user. This requirement should not be confused with an anonymous FTP server. An anonymous FTP server is a special purpose server, which is used to distribute information (e.g., files, educational material, etc.). An anonymous FTP server utilizes an unauthenticated default username such anonymous or ftp and a commonplace password such a "guest." An anonymous FTP server is permitted as long as the server is compliant with the applicable Operating System STIG; is segregated into the network Demilitarized Zone (DMZ), is on its own subnet on a dedicated system, and as long as it only houses "public" information (information approved by the Public Affairs Officer or the equivalent).

- *(EN920: CAT: III) The IAO will ensure an "anonymous" FTP connection within the enclave is not allowed.*

2.11 Enclaves Supporting VoIP and VTC systems

Special consideration must be given to the network security and architecture that supports Voice over IP (VoIP) and Video Teleconferencing (VTC) systems. These systems require a high performance network infrastructure in addition to presenting additional security issues to the network and enclave. These systems inherit all of the vulnerabilities of the network and add some more of their own. The VoIP and VTC systems must be protected from the network vulnerabilities and visa versa. Please refer to the VoIP STIG for the additional security and performance requirements related to these systems.

This page is intentionally left blank.

3. COMPUTING ENVIRONMENT

Computing environment security mechanisms provide the innermost layer of defense for enclaves. The security mechanisms are implemented on the actual end systems including workstations, servers, and mainframes. Computing environment security mechanisms are described in the following sections.

3.1 Operating System (OS) Security

Security features of OSs will be configured in a standardized manner to provide maximum feasible safeguards with the highest level of security possible. These configurations will be periodically checked via an automated mechanism and reapplied, as required. For specific details on OS security configurations, refer to the appropriate OS STIG (e.g., Windows, UNIX, OS/390, etc.).

3.1.1 Gold Disk

With the increasing number of system vulnerabilities, it has become more difficult for SAs and Security Officers to configure and maintain secure information systems. To make it easier, more timely, and consistent with published security policies/guidance, DISA developed a Gold Disk Utility.

The Gold Disk Utility can be used by SAs to assist with the configuration of their Windows and Solaris OSs. It will configure permissions, settings, and install OS patches. The Gold Standard is the base configuration that will be applied by the Gold Disk. Operational impact was considered when establishing the Gold Standard; therefore, providing a high level of assurance that the functioning of the system or installed applications will not be impaired. The Gold Standard is not used for C&A, but is the base level upon which to begin configuring additional requirements for security.

The Gold Disk is being developed in a phased approach with a parallel development schedule that includes a Gold Disk Prototype and Gold Disk Utility. The prototype is a limited functionality utility that will be used until the production Gold Disk Utility is completed. The prototype will perform the basic functions, but will not have the ability to perform a scan of the system before configuration. This functionality is being built into the final Gold Disk Utility.

The production Gold Disk Utility is a GUI-based, security administration tool with both interactive and automatic modes for scanning and fixing identified variations from both the Gold and Platinum standards. The utility will allow SAs to customize security settings that are appropriate for their environment.

3.1.2 Operating System Requirements

- *(EN500: CAT III) The IAO will ensure enclaves use only OSs with an EAL4 or higher rating. OSs that do not contain EAL4 level security features are not used unless justified by a mission requirement and approved by the EMCB or appropriate DAA.*

- *(EN510: CAT II) The IAO will ensure host OSs are configured according to the latest applicable STIG. STIGs provide configuration guidance to achieve an optimal level of security. Operational requirements may prevent implementation of all STIG requirements. In these cases, exceptions are documented as part of the SSAA and approved by the DAA.*

- *(EN520: CAT III) The IAO will ensure major new OS changes are not installed until security guidance is published unless approved by the appropriate DAA. The DAA responds to a request for approval within three months. While guidance is being developed, new OS versions can be loaded for internal testing and evaluation in a Test and Development enclave.*

- *(EN530: CAT III) The IAO will ensure while following the procedures outlined in the DITSCAP, each SSAA includes the OS security requirements in this section as part of the "System Architectural Description" and the "Security Requirements and/or Requirements Traceability Matrix."*

3.1.3 Host-based IDS

A host based intrusion detection system (HIDS) analyzes audit logs for anomalies such as numerous failed logon attempts, activity outside of normal duty hours, and monitor changes to key system files and executables. As there are numerous advantages to a network based intrusion detection system, there are also disadvantages that directly affect the security of the infrastructure. Network based systems cannot detect attacks that do not traverse the network such as attacks from the keyboard of a critical server or other trusted-insider attacks. If an encryption method is employed to encrypt traffic from client to host, a network based IDS will not be able to analyze the traffic. Therefore, intrusion detection must also be provided at the system level to support the DID architecture.

- *(EN540: CAT II) The IAO will ensure all servers employ HIDS, if technically feasible. This requirement may not pertain to legacy systems and cutting edge devices that do not yet have the capability. If a host system cannot technically support a HID, the requirement to employ encryption to the host pursuant to DODI 8500.2 requirements still applies. In these cases, the IAO mitigates the risk by regular review of audit records for these servers. Documentation must exist from the vendor to approve any variance from this requirement.*

- *(EN550: CAT III) The IAO will ensure the SA is responsible for initial response to real-time alarms and perform retrospective analysis of reports.*

- *(EN560: CAT II) The IAO will ensure significant incidents are reported to the site's CNDSP.*

3.1.4 Host-based Content Security Checking

Content Security Checking can also be provided at the host level. In many situations, full content checking at the enclave level may not be possible due to VPN or application layer encryption. In addition, only system-based Content Security Checking can be used to protect workstations from malicious programs that are imported on floppy disks, CD ROMs, Zip drives, tapes, or other removable media.

- *(EN570: CAT I) The IAO will ensure all workstations and servers employ Content Security Checking mechanisms from the DOD-wide anti-virus contract.*

- *(EN580: CAT II) The IAO will ensure Content Security Checking mechanisms are configured to run in a background mode and scan files upon access.*

- *(EN590: CAT I) The IAO will ensure updated virus detection signatures are downloaded and installed, at least every 14 days.*

- *(EN600: CAT IV) The IAM will ensure their organization strongly encourages DOD employees to install the DOD-licensed anti-virus software on the employees' home computers. Organizations should publicize that this software is available free for home use by DOD employees.*

3.2 Application Security

Modern systems supporting DOD operations include a wide range of new technologies that include both new capabilities and new vulnerabilities. The infrastructure services used by these new applications must be secured just as the OSs and networks. Security configuration guidance that is available for some of the infrastructure services supporting typical application developments is described in the following sections.

3.2.1 Internet Applications (Web Servers)

Web servers need to be publicly available, but that very availability exposes them to dishonorable intentions. Common security methods such as firewalls, intrusion detection systems (IDSs), and code integrity checkers do not fully address a web server's particular security needs.

Major security forums (e.g., SANS) have published reports of the Most Critical Internet Security Threats. From these reports, threats unique to web server technology are as follows:

- Default OS and web server software installs and mis-configurations
- Accounts with no passwords, weak passwords, or default passwords
- Non-existent or incomplete backups
- Non-existent or incomplete logging
- Vulnerable CGI programs and application extensions installed on web servers
- Remote Data Services in the Microsoft Internet Information Server (IIS)
- Global file sharing and inappropriate information sharing via NetBIOS and Windows NT ports 135 - 139 (port 445 in Windows 2000), UNIX NFS exports on port 2049, and Macintosh web sharing (AppleShare/IP) on ports 80, 427, and 548

Over the past decade, the Internet has rapidly become a necessary tool for all organizations. Owing to the easy access users have to web sites, web servers have become a focus for those individuals who wish to steal, damage, or deny access to an organization's information and information systems. This is consistent with a trend in malicious user behavior, which focuses on attacking applications accessible via the Internet, as opposed to attacking at the operating system of the host platform. An improperly implemented web server can be attacked directly or be used as a launch point to attack an organization's internal network or other services.

There are many functional areas of Internet and Intranet web technology that must be secured, including the following:

- Network access
- Host operating system
- Web server software
- The application running via the Web server (to include associated scripts and data, the database server, and associated applications
- Information (e.g., account logon data that is transmitted between client and server)
- The client's computer system, most notably the web browser

- *(EN610: CAT III) The IAO will verify that local policies are developed to ensure all originated information posted to the Internet and/or Intranet (i.e., public web servers) is reviewed and approved.*

- *(EN620: CAT II) The IAO will ensure all web servers are configured in compliance with the latest Web Server STIG. Operational requirements may prevent implementation of all STIG requirements. In these cases, extensions are requested from the DAA.*

- *(EN630: CAT III) The IAO will ensure only standard ports are used in accordance with the DOD PPS CAL and the Network Infrastructure STIG.*

- *(EN640: CAT III) The IAO will ensure Public Web servers, approved by the Public Affairs Office (PAO), are isolated on a separate LAN segment (DMZ) from all private DOD systems.*

- *(EN650: CAT II) The IAO will ensure web servers are protected from unauthorized remote access at the enclave perimeter and host levels.*

- *(EN660: CAT II) The IAO will ensure all Internet applications providing encryption, use at a minimum 128-bit SSL encryption and utilize DOD Public Key Infrastructure (PKI) certificates for authentication if technically feasible. (See Table 3-1 below for encryption requirements.)*

Minimum web server authentication requirements are specified in the table below. There are two types of Web servers--Public and Private.

CONTROLS	***SECURITY***	***DESCRIPTIONS***
Public Access can be controlled by IP address or some other means where the restriction is not due to sensitivity.	Unencrypted	Non-sensitive, of general interest to the public, cleared and authorized for public release for which worldwide dissemination poses limited risk for DOD or DOD personnel, even if aggregated with other information reasonably expected to be in the public domain.
Private - User PKI Certificate Server PKI Certificate	Encrypted SSL	Sensitive information that has not been reviewed and approved for release in accordance with DODD 5230.9 and DODI 5230.29.

Table 3-1. Minimum Web Server Authentication Requirements

3.2.2 E-mail Systems

Government-owned, Defense Message System (DMS) approved e-mail systems will be used for authorized U.S. Government business. Unapproved accounts, such as HOTMAIL or YAHOO, will not be used for official business unless specifically authorized to do so by the GIG Waiver Panel. Internet Service Provider (ISP) or web-based commercial e-mail systems will be approved only when it is mission essential and government owned e-mail systems are not available. When approved, users will take special precautions to ensure that any sensitive and/or classified information is not released.

- *(EN670: CAT I) The IAO will ensure classified information is not transmitted over any communications system unless it is transmitted using approved NSA security devices in addition to approved security procedures and practices.*

- *(EN680: CAT I) The IAO will ensure all mail connections to and from mail servers used for anonymous mail redirection are blocked. Mail should be traceable to an individual and known servers. Any servers that have the capability for anonymous mail redirection pose a threat to DOD systems and staff without the possibility of attribution.*

- *(EN690: CAT II) The IAO will ensure all mail systems are configured to block attachments in accordance with the Network Infrastructure STIG, the NSA Guide to E-mail Security in the Wake of Recent Malicious Code Incidents, and the NSA E-mail and Executable Content Guides.*

3.2.3 Mobile Code

Mobile Code is the term given to software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system. An example would be a workstation or laptop, where the recipient executes the web browser without manual installation or initiation of execution by the recipient. Mobile code, such as JavaScript and ActiveX, is particularly vulnerable to malicious attacks. Mobile code is a powerful tool used by developers to run mini-applications or scripts, and they are somewhat easily altered.

- **Category 1 (Active X and Postscript).** Technologies in Category 1 exhibit a broad functionality allowing unmediated access to host and remote system services. Category 1 technologies have known security exploits with few or no countermeasures once access is gained.

- **Category 2 (Java, MS Office VBA, Lotus, PerfectScript).** Category 2 Mobile Code technologies have partial functionality allowing mediated access and environment-controlled access to host system services. Category 2 technologies may have known security exploits, but also have known fine-grained, periodic, or continuous countermeasures/safeguards.

- **Category 3 (JavaScript and PDF).** Technologies in Category 3 support limited functionality, with no capability for direct access to host system services. Category 3 technologies may have a history of known exploits, but also support fine-grained, periodic, or continuous security safeguards. Category 3 technologies may be used in DOD ISs.

- **Non-Categorized Mobile Code Technologies.** Owing to the uncertain risk, Non-Categorized Mobile Code Technologies are prohibited unless explicitly authorized by the DOD CIO Control Board. This technology category will be blocked by all means available at the enclave boundary, workstation, and application layer.

- *(EN700: CAT I) The IAO will ensure Category 1 and non-categorized mobile code is blocked at the enclave perimeter unless signed from a trusted source and approved.*

- *(EN710: CAT III) The IAO will ensure the DODI 8550.cc, Use of Mobile Code Technologies in DOD Information Systems, is adhered to.*

3.2.4 Database Applications

Databases are used to define, store, and manipulate data. A Database Management System (DBMS) supports distributed applications with security services integrated into the DBMS. This shifting of security functions out of the OS requires implementation of a security policy within the database itself. Security controls such as password policy, auditing, Discretionary Access Control (DAC), and role-based access must be configured in the DBMS consistent with the OS security policy. To ensure integrity, confidentiality, and availability of the data that the DBMS controls, security must be first and foremost in the development lifecycle of the system.

- *(EN730: CAT II) The IAO will ensure all DBMSs are configured in compliance with the latest Database STIG.*

Refer to the *Database STIG* for requirements and guidance on DBMS.

3.3 Wireless Devices

Wireless technologies can provide significant productivity improvements for mobile DOD employees; however, they can also expose government information systems to severe security vulnerabilities. Therefore the use of wireless technology must be approved by the individual agency. The security function of the wireless 802.11 standard is inadequate, leading to attacks such as “war driving” and “drive by hacking.” Frequent warnings and advisories have demonstrated the inherent security flaws in the Wired Equivalent Privacy (WEP) standard, which is part of the 802.11 protocol suite. Wireless communication spans a wide range of different technologies including fixed microwave links, wireless LANs, data over cellular networks, wireless WANs, satellite links, digital dispatch networks, and more.

Wireless technologies can be divided into several categories to include fixed, mobile, and portable. Fixed wireless systems are typically located in homes and offices where specialized modems provide connectivity to the Internet. IR wireless uses devices that send data using IR radiation. Portable and mobile wireless systems include devices such as cell phones and Personal Digital Assistants (PDAs) and primarily operate using autonomous battery power.

- *(EN735: CAT II) The IAO will ensure wireless LANs and devices are configured in accordance with the Wireless STIG.*

- *(EN740: CAT II) The IAO will ensure additional encryption, beyond WEP, is employed, such as encrypted VPN, SSL, or SSH.*

- *(EN750: CAT III) The IAO will ensure all services not needed for operational use are disabled on wireless clients.*

- *(EN760: CAT III) The IAO will ensure a user does not install wireless hardware or software or otherwise alter the configuration on government-controlled devices for connecting to a wireless network without prior approval.*

- *(EN770: CAT II) The IAO will ensure personally owned wireless devices are not used for remote access to government systems.*

- *(EN780: CAT I) The only approved wireless technology for the SIPRNET is SecNet-11. The IAO will ensure that the DAA is notified before installation and operation of WLANs intended for use in processing or transmitting classified data, including the SecNet-11. (Refer to the Wireless STIG for details and guidance.)*

- *(EN785: CAT III) The IAO will ensure a policy is in place to periodically scan for rogue wireless devices.*

Refer to the *Wireless STIG* and the *DOD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DOD Global Information Grid (*GIG), for additional guidance and configuration requirements of PDAs and wireless LAN devices.

4. VULNERABILITY ASSESSMENTS

An ongoing program for vulnerability assessments is a key aspect of Phase IV, Post Accreditation Compliance Validation, specified in the DITSCAP. A combination of independent vulnerability assessments and ongoing self-assessments will be used to ensure the controls listed above are properly maintained. The assessments will include both host-based SRRs and penetration tests.

Consequently, conducting periodic vulnerability scans as well as self-assessments will enable sites to find and close vulnerabilities prior to exploitation. These scans need to be conducted on a regular basis, such as quarterly, or even monthly for sensitive networks, and when major network changes are implemented.

- *(EN790: CAT III) The IAO will ensure the SAs operate and maintain online automated vulnerability assessment tools for each system on their network, including systems managed remotely by other organizations. The IAO will ensure the output of these tools is reviewed at least weekly.*

- *(EN800: CAT III) The network manager will coordinate access for random external SIPRNet assessments with the SIPRNet Program Management Office.*

This page is intentionally left blank.

5. SOFTWARE DEVELOPMENT GUIDANCE

5.1 Purpose

The following sections outline basic guidance for software developers who incorporate security mechanisms into new applications that pass traffic between network boundaries. Applications should be developed in a manner that supports the integrity of the internal and external connectivity provided by firewalls. Additionally, applications should not require configurations in the firewall that would negate the effectiveness of the firewall.

5.2 Recommendations

The recommendations in the following sections provide general guidance for integration of security in applications that need access through a firewall. This includes development guidance for protocols, OSs, and encryption.

The *"Recommended Standard Application Security Requirements"* and the *"Application Developer's Security Guidance"* developed by the Applications and Computing Security Division, Center for Information Assurance Applications may be obtained from the https://iase.disa.mil web site. These documents address applications of various types, including Web applications and Web applications that interoperate with backend databases and other legacy servers. The documents discuss ways to avoid general vulnerabilities and common programming and coding errors as well as development methodologies and techniques on ways to ensure that security mechanisms are implemented in applications early in the development life cycle.

- *(EN805: CAT II) The IAO will ensure the application infrastructure is in compliance with the Application Security Checklist.*

5.3 Ports and Protocols

Secure protocols will be used when additional assurance is necessary by the nature of the application or when establishing management sessions with a particular device. If authentication through the firewall is necessary, it will use, at a minimum, a NIST approved FIPS 140-2 encryption algorithm, if the data is sensitive in nature, and supports strong two-factor authentication.

- *(EN810: CAT III) The application developer will ensure only ports and protocols approved by the DOD Ports, Protocols, and Services Assurance Category Assignments List are used.*

- *(EN820: CAT III) The application developer will ensure applications that use new protocols or ports are submitted to the appropriate approving authority for that organization, which in turn are submitted through the PPSMP.*

- *(EN830: CAT III) The application developer will ensure protocols do not use random ports or non-fixed port numbers on servers. Instead, static port allocation should be used to avoid proliferation of possible vulnerabilities.*

- *(EN840: CAT III) The application developer will not modify any IP services and will ensure that each application is compliant to the relevant Request For Comments (RFC) standard.*

- *(EN850: CAT II) The application developer will not write code that requires clients to perform IP forwarding.*

APPENDIX A. NETWORK OPERATIONS CENTER (NOC) ENCLAVE REQUIREMENTS

This is a placeholder for specific requirements for NOC enclaves.

This page is intentionally left blank.

APPENDIX B. DATA CENTER ENCLAVE REQUIREMENTS

This appendix is located in a standalone document due to the sensitivity of the data.

APPENDIX C. TEST AND DEVELOPMENT (LAB) ENCLAVE REQUIREMENTS

This is a placeholder for specific requirements for Test and Development (LAB) enclaves.

This page is intentionally left blank.

APPENDIX D. LIST OF ACRONYMS

ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
AIS	Automated Information System
ANI	Automatic Number Identification
ASD	Assistant Secretary of Defense
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
C/S/A	Combatant Commands/Services/Agencies
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
CC	Common Criteria
CAL	Category Assignments List
CAP	Connection Approval Process
CERT	Computer Emergency Response Team
CIM	Corporate Information Management
CINC	Commander-in-Chief
CIO	Chief Information Officer
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CJCSM	Chairman, Joint Chiefs of Staff Manual
CNA	Computer Network Attack
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
COE	Common Operating Environment
COI	Community of Interest
COMSEC	Communications Security
COOP	Continuity of Operations
COTS	Commercial-Off-The Shelf
CUI	Controlled Unclassified Information
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DBMS	Database Management System
DDoS	Distributed Denial of Service
DECC	Defense Enterprise Computing Center
DECC-D	Defense Enterprise Computing Center-Detachment
DES	Data Encryption Standard
DFAS	Defense Finance and Accounting Service
DID	Defense-in-Depth
DIAP	Defense-Wide Information Assurance Program
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency Instruction
DISN	Defense Information Systems Network
DITSCAP	DOD Information Technology Security Certification and Accreditation Process

DLA	Defense Logistics Agency
DMS	Defense Message System
DMZ	Demilitarized Zone
DNS	Domain Name Service
DNSSEC	DNS Security Extension
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DoS	Denial of Service
DSAWG	DISN Security Accreditation Working Group
EAL	Evaluation Assurance Level
EMCB	Enclave Management Control Board
ESP	Encapsulating Security Payload
FA	Firewall Administrator
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
FSO	Field Security Operations
FTP	File Transfer Protocol
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GNC	Global Network Center
GIG	Global Information Grid
GOTS	Government-off-the Shelf
HID	Host Intrusion Detection
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over Secure Sockets Layers
I&A	Identification and Authentication
IA	Information Assurance
IACB	Information Assurance Control Board
IASE	Information Assurance Support Environment
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IATO	Interim Authority To Operate
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IDS	Intrusion Detection System
IG	Inspector General
IMAP	Internet Mail Access Protocol
INFOCON	Information Operations Condition
INFOSEC	Information Systems Security
IO	Information Operations
IP	Internet Protocol
IPSEC	Internet Protocol Security
IRC	Internet Relay Chat
IS	Information System

ISO	International Standards Organization
ISP	Internet Service Provider
ISSP	Information Systems Security Program
IT	Information Technology
ITM	Information Technology Management
JID	Joint Intrusion Detection
JIEO	Joint Interoperability & Engineering Organization
JTF-GNO	Joint Task Force – Global Network Operations
JWICS	Joint Worldwide Intelligence Communications System
KMP	Key Management Protocol
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCC	Local Control Center
LDAP	Lightweight Directory Access Protocol
MAC	Mission Assurance Category
MD5	Message Digest 5
MPLS	Multiprotocol Label Switching
MVS	Multiple Virtual Storage
NAT	Network Address Translation
NCS	National Communications System
NFS	Network File Server
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NID	Network Intrusion Detection
NIPRNet	Un-Classified Internet Protocol Router Network
NNTP	Net News Transfer Protocol
NOC	Network Operations Center
NSA	National Security Agency
NTP	Network Time Protocol
OS	Operating System
OSI	Open System Interconnection
PAO	Public Affairs Office
PC	Personal Computer
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PE	Processing Element
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POC	Point of Contact
POP	Post Office Protocol
PPP	Point-to-Point Protocol
PPS	Ports, Protocols, and Services

PPTP	Point to Point Tunneling Protocol
RAS	Remote Access Server
RCERT	Regional Computer Emergency Response Team
RFC	Request For Comments
RPC	Remote Procedure Call
SA	System Administrator
SABI	Secret and Below Interoperability
SCIF	Sensitive Compartmented Information Facility
SET	Secure Electronic Transaction
SFTF	Simple File Transfer Protocol
SHA	Secure Hash Algorithm
SIPRNet	Secret Internet Protocol Router Network
SMC	System Management Center
SMI	Security Management Infrastructure
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SRR	Security Readiness Review
SSAA	System Security Authorization Agreement
SSH	Secure Shell
SSL	Secure Socket Layers
STIG	Security Technical Implementation Guide
SUS	Software Update Service
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UID	User Identification
URL	Universal Resource Location
VCTS	Vulnerability Compliance and Tracking System
VLAN	Virtual Local Area Network
VMS	Vulnerability Management System
VOIP	Voice over IP
VPN	Virtual Private Network
VTC	Video Teleconferencing
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WWW	World Wide Web